A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources*

Ming Zhang[1], Zizhan Zheng[2], and Ness B. Shroff[1]

[1] Department of ECE and CSE
The Ohio State University
Columbus,OH,USA
{zhang.2562,shroff.11}@osu.edu
[2] Department of Computer Science
University of California, Davis
Davis,CA,USA
cszheng@ucdavis.edu

Abstract. Stealthy attacks are a major threat to cyber security. In practice, both attackers and defenders have resource constraints that could limit their capabilities. Hence, to develop robust defense strategies, a promising approach is to utilize game theory to understand the fundamental trade-offs involved. Previous works in this direction, however, mainly focus on the single-node case without considering strict resource constraints. In this paper, a game-theoretic model for protecting a system of multiple nodes against stealthy attacks is proposed. We consider the practical setting where the frequencies of both attack and defense are constrained by limited resources, and an asymmetric feedback structure where the attacker can fully observe the states of nodes while largely hiding its actions from the defender. We characterize the best response strategies for both attacker and defender, and study the Nash Equilibria of the game. We further study a sequential game where the defender first announces its strategy and the attacker then responds accordingly, and design an algorithm that finds a nearly optimal strategy for the defender to commit to.

Keywords: Stealthy Attacks, Resource Constraints, Game Theory

1 Introduction

The landscape of cyber security is constantly evolving in response to increasingly sophisticated cyber attacks. In recent years, *Advanced Persistent Threats* (APT) [1] is becoming a major concern to cyber security. APT attacks have several distinguishing properties that render traditional defense mechanism less effective. First, they are often launched by *incentive driven* entities with specific targets. Second, they are *persistent* in achieving the goals, and may involve multiple stages or continuous operations over a long period of time. Third, they are

* This work has been funded by QNRF fund NPRP 5-559-2-227 and ARO-W911NF-15-1-0277.

highly adaptive and *stealthy*, and often operate in a "low-and-slow" fashion [7] to avoid of being detected. In fact, some notorious attacks remained undetected for months or longer [2,6]. Hence, traditional intrusion detection and prevention techniques that target one-shot and known attack types are insufficient in the face of long-lasting and stealthy attacks.

Moreover, since the last decade, it has been increasingly realized that security failures in information systems are often caused by the misunderstanding of incentives of the entities involved in the system instead of the lack of proper technical mechanisms [5, 18]. To this end, game theoretical models have been extensively applied to cyber security [4, 9–11, 14, 17, 20]. Game theory provides a proper framework to systematically reason about the strategic behavior of each side, and gives insights to the design of cost-effective defense strategies. Traditional game models, however, fail to capture the persistent and stealthy behavior of advanced attacks. Further, they often model the cost of defense (or attack) as part of the utility functions of the players, while ignoring the strict resource constraints during the play of the game. For a large system with many components, ignoring such constraints can lead to either over-provision or under-provision of resources and revenue loss.

In this paper, we study a two-player non-zero-sum game that explicitly models stealth attacks with resource constraints. We consider a system with N *independent* nodes (or components), an attacker, and a defender. Over a continuous time horizon, the attacker (defender) determines when to attack (recapture) a node, subject to a unit cost per action that varies over nodes. At any time t, a node is either compromised or protected, depending on whether the player that makes the last move (i.e., action) towards it before t is the attacker or the defender. A player obtains a value for each node under its control per unit time, which again may vary over nodes. The total payoff to a player is then the total value of the nodes under its control over the entire time horizon minus the total cost incurred, and we are interested in the long-term time average payoffs.

To model stealthy attacks, we assume that the defender gets no feedback about the attacker during the game. On the other hand, the defender's moves are fully observable to the attacker. This is a reasonable assumption in many cyber security settings, as the attacker can often observe and learn the defender's behavior before taking actions. Moreover, we explicitly model their resource constraints by placing an upper bound on the frequency of moves (over all the nodes) for each player. We consider both Nash Equilibrum and Sequential Equilibrum for this game model. In the latter case, we assume that the defender is the leader that first announces its strategy, and the attacker then responds with its best strategy. The sequential setting is often relevant in cyber security, and can provide a higher payoff to the defender compared with Nash Equilibrum. To simplify the analysis, we assume that the set of nodes are independent in the sense that the proper functioning of one node does not depend on other nodes, which serves as a first-order approximation of the more general setting of interdependent nodes to be considered in our future work.

Our model is an extension of the asymmetric version of the FlipIt game considered in [16]. The FlipIt game [21] is a two-player non-zero-sum game recently proposed in response to an APT attack towards RSA Data Security [3]. In the FlipIt game, a single critical resource (a node in our model) is considered. Each player obtains control over the resource by "flipping" it subject to a cost. During the play of the game, each player obtains delayed and possibly incomplete feedback on the other player's previous moves. A player's strategy is then when to move over a time horizon, and the solution of the game heavily depends on the class of strategies adopted and the feedback structure of the game. In particular, a full analysis of Nash Equilibria has only been obtained for two special cases, when both players employ a periodic strategy [21], and when the attacker is stealthy and the defender is observable as in our model [16]. However, both works consider a single node and there is no resource constraint. The multi-node setting together with the resource constraints impose significant challenges in characterizing both Nash and Sequential Equilibria. A different multi-node extension of the FlipIt game is considered in [15] where the attacker needs to compromise either all the nodes (AND model) or a single node (OR model) to take over a system. However, only preliminary analytic results are provided.

Our game model can be applied in various settings. One example is key rotation. Consider a system with multiple nodes, e.g., multiple communication links or multiple servers, that are protected by different keys. From time to time, the attacker may compromise some of the keys, e.g., by leveraging zero-day vulnerabilities and system specific knowledge, while remaining undetected from the defender. A common practice is to periodically generate fresh keys by a trusted key-management service, without knowing when they are compromised. On the other hand, the attacker can easily detect the expiration of a key (at an ignorable cost compared with re-compromising it). Both key rotation and compromise incurs a cost, and there is a constraint on the frequency of moves at each side. There are other examples where our extension of the FlipIt game can be useful, such as password reset and virtual-machine refresh [8, 16, 21].

We have made following contributions in this paper.

- We propose a two-player game model with multiple independent nodes, an overt defender, and a stealthy attacker where both players have strict resource constraints in terms of the frequency of protection/attack actions across all the nodes.
- We prove that the periodic strategy is a best-response strategy for the defender against a non-adaptive *i.i.d.* strategy of the attacker, and vice versa, for general distributions of attack times.
- For the above pair of strategies, we fully characterize the set of Nash Equilibria of our game, and show that there is always one (and maybe more) equilibrium, for the case when the attack times are deterministic.
- We further consider the sequential game with the defender as the leader and the attacker as the follower. We design a dynamic programming based algorithm that identifies a nearly optimal strategy (in the sense of subgame perfect equilibrium) for the defender to commit to.

The remainder of this paper is organized as follows. We present our game-theoretic model in Section 2, and study best-response strategies of both players in Section 3. Analysis of Nash Equilibria of the game is provided in Section 4, and the sequential game is studied in Section 5. In Section 6, we present numerical result, and we conclude the paper in Section 7.

2 Game Model

In this section, we discuss our two-player game model including its information structure, the action spaces of both attacker and defender, and their payoffs. Our game model extends the single node model in [16] to multiple nodes and includes a resource constraint to each player.

2.1 Basic Model

In our game-theoretical model, there are two players and N *independent* nodes [3]. The player who is the lawful user/owner of the N nodes is called the defender, while the other player is called the attacker. The game starts at time $t = 0$ and goes to any time $t = T$. We assume that time is continuous. A player can make a move at any time instance subject to a cost per move. At any time t, a node is under the control of the player that makes the last move towards the node before t (see Figure 1). Each attack towards node i incurs a cost of C_i^A to the attacker, and it takes a random period of time w_i to succeed. On the other hand, when the defender makes a move to protect node i, which incurs a cost of C_i^D, node i is recovered immediately even if the attack is still in process. Each node i has a value r_i that represents the benefit that the attacker receives from node i per unit of time when node i is compromised.

In addition to the move cost, we introduce a strict resource constraint for each player, which is a practical assumption but has been ignored in most prior works on security games. In particular, we place an upper bound on the average amount of resource that is available to each player at any time (to be formally defined below). As typical security games, we assume that r_i, C_i^A, C_i^D, the distribution of w_i, and the budget constraints are all common knowledge of the game, that is, they are known to both players. For instance, they can be learned from history data and domain knowledge. Without loss of generality, all nodes are assumed to be protected at time $t = 0$. Table 1 summarizes the notations used in the paper.

As in [16], we consider an asymmetric feedback model where the attacker's moves are *stealthy*, while the defenders' moves are *observable*. More specifically, at any time, the attacker knows the full history of moves by the defender, as well as the state of each node, while the defender has no idea about whether a node is compromised or not. Let $\alpha_{i,k}$ denote the time period the attacker waits from the latest time when node i is recovered, to the time when the attacker starts

[3] The terms "components" and "nodes" are interchangeable in this paper.

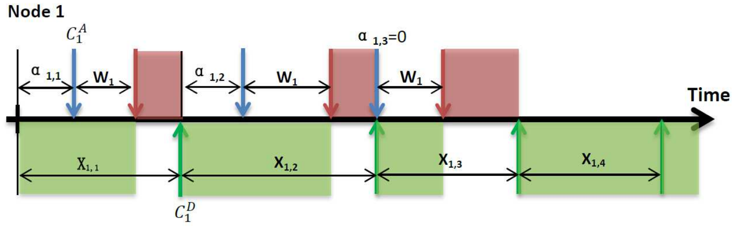


Fig. 1: Game Model

Table 1: List of Notations

Symbol	Meaning
T	time horizon
N	number of nodes
r_i	value per unit of time of compromising node i
w_i	attack time for node i
C_i^A	attacker's move cost for node i
C_i^D	defender's move cost for node i
$\alpha_{i,k}$	attacker's waiting time in its k-th move for node i
$X_{i,k}$	time between the (k-1)-th and the k-th defense for node i
B	budget to the defender, greater than 0
M	budget to the attacker, greater than 0
m_i	frequency of defenses for node i
p_i	probability of immediate attack on node i once it recovers
L_i	the number of defense moves for node i

its k-th attack against node i, which can be a random variable in general. The attacker's action space is then all the possible selections of $\{\alpha_{i,k}\}$. Since the set of nodes are independent, we can assume $\alpha_{i,k}$ to be independent across i without loss of generality. However, they may be correlated across k in general, as the attacker can employ a time-correlated strategy. On the contrary, the defender's strategy is to determine the time intervals between its $(k-1)$-th move and k-th move for each node i and k, denoted as $X_{i,k}$.

In this paper, we focus on *non-adaptive (but possibly randomized) strategies*, that is, neither the attacker nor the defender changes its strategy based on feedback received during the game. Therefore, the values of $\alpha_{i,k}$ and $X_{i,k}$ can be determined by the corresponding player before the game starts. Note that assuming non-adaptive strategies is not a limitation for the defender since it does not get any feedback during the game anyway. Interestingly, it turns out not to be a big limitation on the attacker either. As we will show in Section 3, periodic defense is a best-response strategy against any non-adaptive *i.i.d.* attacks (formally defined in Definition 2) and vice versa. Note that when the defender's strategy is periodic, the attacker can predict defender's moves before the game starts so there is no need to be adaptive.

2.2 Defender's Problem

Consider a fixed period of time T and let L_i denote the total number of defense moves towards node i during T. L_i is a random variable in general. The total amount of time when node i is compromised is then $T - \sum_{k=1}^{L_i} \min(\alpha_{i,k} + w_i, X_{i,k})$. Moreover, the cost for defending node i is $L_i C_i^D$. The defender's payoff is then defined as the total loss (non-positive) minus the total defense cost over all the nodes. Given the attacker's strategy $\{\alpha_{i,k}\}$, the defender faces the following optimization problem:

$$\begin{aligned} \max_{\{X_{i,k}\}, L_i} \; & E\left[\sum_{i=1}^{N} \frac{-\left(T - \sum_{k=1}^{L_i} \min(\alpha_{i,k} + w_i, X_{i,k})\right) \cdot r_i - L_i C_i^D}{T}\right] \\ s.t. & \sum_{i=1}^{N} \frac{L_i}{T} \leq B \text{ w.p.1} \\ & \sum_{k=1}^{L_i} X_{i,k} \leq T \text{ w.p.1 } \forall i \end{aligned} \tag{1}$$

The first constraint requires that the average number of nodes that can be protected at any time is upper bounded by a constant B. The second constraint defines the feasible set of $X_{i,k}$. Since T is given, the expectation in the objective function can be moved into the summation in the numerator.

2.3 Attacker's Problem

We again let L_i denote the total number of defense moves towards node i in T. The total cost of attacking i is then $(\sum_{k=1}^{L_i} \mathbf{1}_{\alpha_{i,k} < X_{i,k}}) \cdot C_i^A$, where $\mathbf{1}_{\alpha_{i,k} < X_{i,k}} = 1$ if $\alpha_{i,k} < X_{i,k}$ and $\mathbf{1}_{\alpha_{i,k} < X_{i,k}} = 0$ otherwise. It is important to note that when $\alpha_{i,k} \geq X_{i,k}$, the attacker actually gives up its k-th attack against node i (this is possible as the attacker can observe when the defender moves). Given the defender's strategy, the attacker's problem can be formulated as follows, where M is an upper bound on the average number of nodes that the attacker can attack at any time instance.

$$\begin{aligned} \max_{\alpha_{i,k}} \quad & E\left[\sum_{i=1}^{N} \frac{(T - \sum_{k=1}^{L_i} \min(\alpha_{i,k} + w_i, X_{i,k})) \cdot r_i - (\sum_{k=1}^{L_i} \mathbf{1}_{\alpha_{i,k} < X_{i,k}}) \cdot C_i^A}{T}\right] \\ s.t. \quad & E\left[\sum_{i=1}^{N} \frac{1}{T} \int_0^T v_i(t) dt\right] \leq M \end{aligned} \tag{2}$$

where $v_i(t) = 1$ if the attacker is attacking node i at time t and $v_i(t) = 0$ otherwise. Note that we make the assumption that the attacker has to keep consuming resources when the attack is in progress instead of making an instantaneous move like the defender; hence it has a different form of budget constraint.

On the other hand, we assume that C_i^A captures the total cost for each attack on node i, which is independent of the attack time. We further have the following equation:

$$\int_0^T v_i(t)dt = \sum_{k=1}^{L_i} (\min(\alpha_{i,k} + w_i, X_{i,k}) - \min(\alpha_{i,k}, X_{i,k})) \tag{3}$$

Putting (3) into (2) and moving the expectation inside, the attacker's problem becomes

$$\begin{aligned} &\max_{\alpha_{i,k}} \sum_{i=1}^{N} \frac{T \cdot r_i - E[\sum_{k=1}^{L_i} \min(\alpha_{i,k} + w_i, X_{i,k})] \cdot r_i - E[\sum_{k=1}^{L_i} P(\alpha_{i,k} < X_{i,k})] \cdot C_i^A}{T} \\ &s.t. \sum_{i=1}^{N} \frac{E[\sum_{k=1}^{L_i} \min(\alpha_{i,k} + w_i, X_{i,k}) - \min(\alpha_{i,k}, X_{i,k})]}{T} \leq M \end{aligned} \tag{4}$$

3 Best Responses

In this section, we analyze the best-response strategies for both players. Our main result is that when the attacker employs a non-adaptive *i.i.d.* strategy, a periodic strategy is a best response for the defender, and vice versa. To prove this result, however, we have provided characterization of best responses in more general settings.

3.1 Defender's Best Response

We first show that for the defender's problem (1), an optimal deterministic strategy is also optimal in general. We then provide a sufficient condition for a deterministic strategy to be optimal against any non-adaptive attacks. Finally, we show that periodic defense is optimal against non-adaptive *i.i.d.* attacks.

Lemma 1. *Suppose $X_{i,k}^\star$ and $L_i^\star$ are the optimal solutions of* (1) *among all deterministic strategies, then they are also optimal among all the strategies including both deterministic and randomized strategies.*

Proof. Define $x_{i,k}$ and l_i as the realization of $X_{i,k}$ and L_i respectively and let $\mathcal{C} = \{[x_{i,k}\ l_i] | \sum_{i=1}^N \frac{l_i}{T} \leq B$ *and* $\sum_{k=1}^{l_i} x_{i,k} \leq T\}$. Then, we denote $U^D(X_{i,k}, L_i)$ as the target function of (1) and denote

$$\begin{aligned} &\hat{U}^D(x_{i,k}, l_i) \\ &= \sum_{i=1}^{N} \frac{-\left(T - \sum_{k=1}^{l_i} E[\min(\alpha_{i,k} + w_i, x_{i,k})]\right) \cdot r_i - l_i C_i^D}{T} \end{aligned} \tag{5}$$

Now, for any $[X_{i,k}\ L_i] \in \mathcal{C}\ w.p.1$, we have

$$\begin{aligned}
&U^D(X_{i,k}, L_i)\\
&= P(X_{i,k} = X^\star_{i,k}\ L_i = L^\star_i,\ \forall i, k) \cdot \hat{U}^D(X^\star_{i,k}, L^\star_i)\\
&+ \sum_{\substack{[x_{i,k}\ \ l_i]\in\mathcal{C}\\ x_{i,k}\neq X^\star_{i,k}\ \ l_i\neq L^\star_i}} P(X_{i,k} = x_{i,k}\ L_i = l_i,\ \forall i, k) \cdot \hat{U}^D(x_{i,k}, l_i)\\
&\leq \hat{U}^D(X^\star_{i,k}, L^\star_i)
\end{aligned} \tag{6}$$

The equality holds only when $X_{i,k} = X^\star_{i,k}\ L_i = L^\star_i\ \forall i, k\ w.p.1$. Therefore, $X^\star_{i,k}$ and $L^\star_i$ are also optimal among all the defender's strategies. □

According to the lemma, it suffices to consider defender's strategies where both $X_{i,k}$ and $L_{i,k}$ are deterministic.

Definition 1. *For a given L_i, we define a set $\mathcal{X}_i$ including all deterministic defense strategies with the following properties:*

1. $\sum_{k=1}^{L_i} X_{i,k} = T$;
2. $F_{\alpha_{i,k}+w_i}(X_{i,k}) = F_{\alpha_{i,j}+w_i}(X_{i,j})\ \ \forall k, j$,

where $F_{\alpha_{i,k}+w_i}(\cdot)$ is the CDF of r.v. $\alpha_{i,k} + w_i$.

Note that $\mathcal{X}_i$ can be an empty set in general due to the randomness of $\alpha_{i,k} + w_i$. The following lemma shows that when $\mathcal{X}_i$ is non-empty for all i, any strategy that belongs to $\mathcal{X}_i$ is the defender's best deterministic strategy against a non-adaptive attacker.

Lemma 2. *For any given set of $\{L_i\}$ with $\sum_{i=1}^{N} \frac{L_i}{T} \leq B$, if $\mathcal{X}_i \neq \emptyset\ \forall i$, then any set of $\{X_{i,k}\}$ which belongs to $\mathcal{X}_i$, is the defender's best deterministic strategy.*

Proof. We first define the defender's payoff for node i as

$$U^D_i(X_{i,k}, L_i) = \frac{-\left(T - \sum_{k=1}^{L_i} E[\min(\alpha_{i,k} + w_i, X_{i,k})]\right) \cdot r_i - L_i C^D_i}{T}. \tag{7}$$

Since $\{L_i\}$ are fixed, Problem (1) can be divided into N independent subproblems as follows:

$$\begin{aligned}
&\max_{X_{i,k}} U^D_i(X_{i,k})\\
&s.t. \sum_{k=1}^{L_i} X_{i,k} \leq T
\end{aligned} \tag{8}$$

Take double derivatives of $U^D_i(\{X_{i,k}\})$ with respect to X_i, we have

$$\frac{\partial^2 U^D_i(X_{i,k})}{\partial X_i^2} = \begin{pmatrix}
-\frac{f_{\alpha_{i,k}+w_i}(X_{i,1})}{T} & 0 & \cdots & 0\\
0 & -\frac{f_{\alpha_{i,k}+w_i}(X_{i,2})}{T} & \cdots & 0\\
\vdots & \vdots & \ddots & \vdots\\
0 & 0 & \cdots & -\frac{f_{\alpha_{i,k}+w_i}(X_{i,L_i})}{T}
\end{pmatrix} \tag{9}$$

where $f_{\alpha_{i,k}+w_i}(\cdot)$ is the *p.d.f.* of r.v. $\alpha_{i,k}+w_i$.

It follows that the objective function is concave because the above matrix is a non-positive definite matrix. Here, we assume that $F_{\alpha_{i,k}+w_i}(X_{i,k})$ is continuous. However, the concavity can still be proved in general using the subgradient concept. Since $U_i^D(X_{i,k})$ is concave and continuously differentiable, the KKT conditions are both sufficient and necessary. From the KKT conditions, we have $\nu^\star(\sum_{k=1}^{L_i} X_{i,k} - T) = 0$ and $F_{\alpha_{i,k}+w_i}(X_{i,k}) = F_{\alpha_{i,j}+w_i}(X_{i,j}), \forall k, j$, where $\nu^\star$ is the Lagrangian multiplier. It is clear that $U_i^D(X_{i,k})$ is maximized when the constraint is tight, that is, $\sum_{k=1}^{L_i} X_{i,k} = T$. However, there may exist a set of $X_{i,k}$ s.t. $\sum_{k=1}^{L_i} X_{i,k} < T$ but it is still optimal for (8). Thus, the two conditions in Definition 1 are only sufficient. □

Lemma 2 gives a sufficient condition for a deterministic defense strategy to be optimal. The main idea of the proof is to show that the defender's payoff for each node i is concave with respect to $X_{i,k}$. The optimality then follows from the KKT conditions. Intuitively, the defender tries to equalize its expected loss in each period in a deterministic way, which gives the defender the most stable system to avoid a big loss in any particular period. We then show that a periodic defense is sufficient when the attacker employs a non-adaptive *i.i.d.* strategy formally defined below.

Definition 2. *An attack strategy is called non-adaptive i.i.d. if it is non-adaptive, and $\alpha_{i,k}$ is independent across i and is i.i.d. across k.*

Theorem 1. *A periodical strategy is the best response for the defender if the attacker employs a non-adaptive i.i.d. strategy.*

Proof. For any fixed $\{L_i\}$, let $X_i \triangleq [\frac{T}{L_i}\frac{T}{L_i}\cdots\frac{T}{L_i}]$. It is easy to check that $\{X_i\}$ satisfies the fist property in Definition 1 and will satisfy the second property if $\alpha_{i,k}$ is *i.i.d.* with respect to k. According to Lemma 2, $\{X_i\}$ is an optimal (deterministic) solution respecting $\{L_i\}$. It follows that if we let $\{L_i^\star\}$ denote the optimal solution of

$$\begin{aligned} \max_{L_i} \sum_{i=1}^{N} & \frac{-\left(T - \sum_{k=1}^{L_i} E[\min(\alpha_{i,k}+w_i, \frac{T}{L_i})]\right)\cdot r_i - L_i C_i^D}{T} \\ s.t. & \sum_{i=1}^{N} \frac{L_i}{T} \le B \end{aligned} \tag{10}$$

then $X_i^\star \triangleq [\frac{T}{L_i^\star}\frac{T}{L_i^\star}\cdots\frac{T}{L_i^\star}], \forall i$ is an optimal solutions to the defender's problem. Hence, a periodic strategy with periods of $X_i^\star, \forall i$ is a best-response strategy for the defender. □

According to the theorem, the periodic strategy gives the defender the most stable system when the attacker adopts the non-adaptive *i.i.d.* strategy. Since the attacker's waiting time $\alpha_{i,k}$ does not change with time, a fixed defense interval provides the same expected payoff between every two consecutive moves.

Moreover, since the defender's problem is a convex optimization problem, the optimal defending frequency for a given attack strategy can be easily determined by solving the convex program.

3.2 Attacker's Best Response

We first analyze the attacker's best response against any deterministic defense strategies, then show that the non-adaptive *i.i.d.* strategy is the best response against periodic defense.

Lemma 3. *When defense strategies are deterministic, the attacker's best response (among non-adaptive strategies) must satisfy the following condition*

$$\alpha^{\star}_{i,k} = \begin{cases} 0 & w.p.\ p_{i,k} \\ \geq X_{i,k} & w.p.\ 1 - p_{i,k} \end{cases} \tag{11}$$

Proof sketch: The main idea of the proof is to divide the problem (4) into N independent sub-problems, one for each node, where each subproblem has a similar target function and a budget M_i with $\sum_{i=1}^{N} M_i = M$, as follows (note that we consider an equivalent minimization problem by ignoring the constant term r_i in (4).

$$\begin{aligned} \min_{\alpha_{i,k}} \sum_{k=1}^{L_i} & \frac{E[\min(\alpha_{i,k} + w_i, X_{i,k})] \cdot r_i + P(\alpha_{i,k} < X_{i,k}) \cdot C_i^A}{T} \\ s.t. \sum_{k=1}^{L_i} & \frac{E[\min(\alpha_{i,k} + w_i, X_{i,k})] - E[\min(\alpha_{i,k}, X_{i,k})]}{T} \leq M_i \end{aligned} \tag{12}$$

Each sub-problem is further divided into L_i independent sub-problems with budget $M_{i,k}$ where $\sum_{k=1}^{L_i} M_{i,k} = M_i$. Due to the independence of nodes, it suffices to prove the lemma for any of these sub-problems. The detailed proof is in Section 8.

Lemma 3 implies that for each node i, the attacker's best strategy is to either attack node i immediately after it realizes the node's recovery, or gives up the attack until the defender's next move. There is no incentive for the attacker to wait a small amount of time to attack a node before the defender's next move. The constraint M actually determines the probability that the attacker will attack immediately. If M is large enough, the attacker will never wait after defender's each move. We then find the attacker's best responses when the defender employs the periodic strategy.

Theorem 2. *When the defender employs periodical strategy, the non-adaptive i.i.d. strategy is the attacker's best response among all non-adaptive strategies.*

Proof. If the defender uses periodic strategy where for each i, $X_{i,k} = \frac{1}{m_i}, \forall k$, all $\eta_{i,k}$'s are equal with respect to k. Therefore, setting all $p_{i,k}$ in (11) equal such that $\alpha_{i,k}$ is $i.i.d$ across i, is one of the best solutions for (12) for any given M_i. Since the set of nodes are independent, the non-adaptive *i.i.d.* strategy is also a best solution for (4) when the defender uses periodic strategy. □

3.3 Simplified Optimization Problems

According to Theorem 1 and Theorem 2, periodic defense and non-adaptive *i.i.d.* attack can form a pair of best-response strategies with respect to each other. Consider such pair of strategies. Let $m_i \triangleq \frac{L_i}{T} = \frac{1}{X_{i,k}}$, and let p_i denote the probability that $\alpha_{i,k} = 0, \forall k$. The optimization problems to the defender and the attacker can then be simplified as follows.
Defender's problem:

$$\begin{aligned} \max_{m_i} \sum_{i=1}^{N} & \left[\left(E[\min{(w_i, \frac{1}{m_i})}]p_i r_i - C_i^D \right) \cdot m_i - p_i r_i \right] \\ s.t. & \sum_{i=1}^{N} m_i \leq B \end{aligned} \tag{13}$$

Attacker's problem:

$$\begin{aligned} \max_{p_i} \sum_{i=0}^{N} & p_i \cdot \left(r_i (1 - E[\min(w_i, \frac{1}{m_i})] \cdot m_i) - C_i^A m_i \right) \\ s.t. \sum_{i=0}^{N} & E[\min(w_i, \frac{1}{m_i})] \cdot m_i \cdot p_i \leq M \end{aligned} \tag{14}$$

We observe that the defender's problem is a continuous convex optimization problem (see the discussion in Section 3.1), and the attacker's problem is a fractional knapsack problem. Therefore, the best response strategy of each side can be easily determined. Also, the time period T disappears in both problems.

4 Nash Equilibria

In this section, we study the set of Nash Equilibria of the simplified game as discussed in Section 3.3 where the defender employs a periodic strategy, and the attacker employs a non-adaptive *i.i.d.* strategy. We further assume that the attack time w_i is deterministic for all i. We show that this game always has a Nash equilibrium and may have multiple equilibria of different values.

We first observe that for deterministic w_i, when $m_i \geq \frac{1}{w_i}$, the defender's payoff becomes $-m_i C_i^D$, which is maximized when $m_i = \frac{1}{w_i}$. Therefore, it suffices to consider $m_i \leq \frac{1}{w_i}$. Thus, the optimization problems to the defender and the attacker can be further simplified as follows.

For a given p, the defender aims at maximizing its payoff:

$$\begin{aligned} &\max_{m_i} \sum_{i=1}^{N} [m_i(r_i w_i p_i - C_i^D) - p_i r_i] \\ &s.t. \ \sum_{i=1}^{N} m_i \leq B \\ &\qquad 0 \leq m_i \leq \frac{1}{w_i}, \forall i \end{aligned} \tag{15}$$

On the other hand, for a given m, the attacker aims at maximizing its payoff:

$$\begin{aligned} &\max_{p_i} \sum_{i=1}^{N} p_i[r_i - m_i(r_i w_i + C_i^A)] \\ &s.t. \ \sum_{i=1}^{N} m_i w_i p_i \leq M \\ &\qquad 0 \leq p_i \leq 1, \forall i \end{aligned} \tag{16}$$

For a pair of strategies (m, p), the payoff to the defender is $U_d(m, p) = \sum_{i=1}^{N}[m_i(p_i r_i w_i - C_i^D) - p_i r_i]$, while the payoff to the attacker is $U_a(m, p) = \sum_{i=1}^{N} p_i[r_i - m_i(r_i w_i + C_i^A)]$. A pair of strategies (m^*, p^*) is called a (pure strategy) *Nash Equilibrium (NE)* if for any pair of strategies (m, p), we have $U_d(m^*, p^*) \geq U_d(m, p^*)$ and $U_a(m^*, p^*) \geq U_a(m^*, p)$. In the following, we assume that $C_i^A > 0$ and $C_i^D > 0$. The cases where $C_i^A = 0$ or $C_i^D = 0$ or both exhibit slightly different structures, but can be analyzed using the same approach. Without loss of generality, we assume $r_i > 0$ and $\frac{C_i^D}{r_i w_i} \leq 1$ for all i. Note that if $r_i = 0$, then node i can be safely excluded from the game, while if $\frac{C_i^D}{r_i w_i} > 1$, the coefficient of m_i in U_d (defined below) is always negative and there is no need to protect node i.

Let $\mu_i(p) \triangleq p_i r_i w_i - C_i^D$ denote the coefficient of m_i in U_d, and $\rho_i(m) \triangleq \frac{r_i - m_i(r_i w_i + C_i^A)}{m_i w_i}$. Note that for a given p, the defender tends to protect more a component with higher $\mu_i(p)$, while for a given m, the attacker will attack a component more frequently with higher $\rho_i(m)$. When m and p are clear from the context, we simply let μ_i and ρ_i denote $\mu_i(p)$ and $\rho_i(m)$, respectively.

To find the set of NEs of our game, a key observation is that if there is a full allocation of defense budget B to m such that $\rho_i(m)$ is a constant for all i, any full allocation of the attack budget M gives the attacker the same payoff. Among these allocations, if there is further an assignment of p such that $\mu_i(p)$ is a constant for all i, then the defender also has no incentive to deviate from m; hence (m, p) forms an NE. The main challenge, however, is that such an assignment of p does not always exist for the whole set of nodes. Moreover, there are NEs that do not fully utilize the defense or attack budget as we show below. To characterize the set of NEs, we first prove the following properties satisfied by any NE of the game. For a given strategy (m, p), we define $\mu^*(p) \triangleq \max_i \mu_i(p)$, $\rho^*(m) \triangleq \min_i \rho_i(m)$, $F(p) \triangleq \{i : \mu_i(p) = \mu^*(p)\}$, and $D(m, p) \triangleq \{i \in F : \rho_i(m) = \rho^*(m)\}$. We omit m and p when they are clear from the context.

Lemma 4. *In any NE, (1)* $m_i \leq \frac{r_i}{r_i w_i + C_i^A}$ *and (2)* $p_i \geq \frac{C_i^D}{r_i w_i}$.

Proof. To prove the first property, suppose $m_i > \frac{r_i}{r_i w_i + C_i^A}$. Then p_i must be 0; otherwise the benefit for attacking i becomes negative. This in turn implies that $m_i = 0$ by the assumption that $C_i^D > 0$, a contradiction. To prove the second property, suppose $p_i < \frac{C_i^D}{r_i w_i}$. Then we have $\mu_i < 0$, which implies $m_i = 0$ and therefore $p_i = 1$ since $r_i > 0$, a contradiction. □

Lemma 5. *If* (m, p) *is an NE, we have (see Table 2) :*

1. $\forall i \notin F, m_i = 0, p_i = 1, \rho_i = \infty$;
2. $\forall i \in F \backslash D, m_i \in [0, \frac{r_i}{w_i r_i + C_i^A}], p_i = 1$;
3. $\forall i \in D, m_i \in [0, \frac{r_i}{w_i r_i + C_i^A}], p_i \in [\frac{C_i^D}{r_i w_i}, 1]$.

Proof. We first show that if $m_i > 0$ and $m_j > 0$, then $\mu_i = \mu_j$. Suppose $\mu_i < \mu_j$. Then it is better to protect i than protecting j. Since $m_i > 0$, we must have $m_j = \frac{1}{w_j} > \frac{r_i}{r_i w_i + C_i^A}$ by the assumption that $C_i^A > 0$, a contradiction. It follows that $m_i = 0 \ \forall i \notin F$ and $m_i \in [0, \frac{r_i}{r_i w_i + C_i^A}] \ \forall i \in F$. Since when $m_i = 0$, we must have $\rho_i = \infty$, and $p_i = 1$, $p_i = 1, \rho_i = \infty \ \forall i \notin F$. It remains to show that $p_i = 1$ for all $i \in F \backslash D$. Assuming $F \backslash D \neq \emptyset$, then we have $\rho_j < \infty$ for $j \in D$, which implies that $m_j > 0$ for $j \in D$. Since $\rho_i < \rho^*$ for $i \in F \backslash D$, it is more beneficial to attack i that any $j \in D$. Since $p_j > 0$ and $m_j > 0$ for $j \in D$, we must have $p_i = 1$. □

Lemma 6. *If* (m, p) *forms an NE, then for* $i \in D, j \in F \backslash D$ *and* $k \notin F$*, we have* $r_i w_i - C_i^D \geq r_j w_j - C_j^D > r_k w_k - C_k^D$.

Proof. Since $\mu_i = \mu_j$ for $i \in D$ and $j \in F \backslash D$ by the definitions of F and D, and $p_i \leq p_j = 1$ by Lemma 5, we have $r_i w_i - C_i^D \geq \mu_i = \mu_j \geq r_j w_j - C_j^D$. On the other hand, since $\mu_j > \mu_k$ by the definition of F, and $p_j = p_k = 1$ by Lemma 5, we have $r_j w_j - C_j^D = \mu_j > \mu_k = r_k w_k - C_k^D$. □

According to the above lemma, to find all the equilibria of the game, it suffices to sort all the nodes by a non-increasing order of $r_i w_i - C_i^D$, and consider each F_h consisting of the first h nodes such that $r_h w_h - C_h^D > r_{h+1} w_{h+1} - C_{h+1}^D$, and each subset $D_k \subseteq F_h$ consisting of the first $k \leq h$ nodes in the list. In the following, we assume such an ordering of nodes. Consider a given pair of F and $D \subseteq F$. By Lemma 5 and the definitions of F and D, the following conditions are satisfied by any NE with $F(p) = F$ and $D(m, p) = D$.

$$m_i = 0, p_i = 1, \forall i \notin F; \tag{17}$$

$$m_i \in [0, \frac{r_i}{w_i r_i + C_i^A}], p_i = 1, \forall i \in F \backslash D; \tag{18}$$

$$m_i \in [0, \frac{r_i}{w_i r_i + C_i^A}], p_i \in [\frac{C_i^D}{r_i w_i}, 1], \forall i \in D; \tag{19}$$

$$\sum_{i \in F} m_i \leq B, \sum_{i \in F} m_i w_i p_i \leq M; \tag{20}$$

$$\mu_i = \mu^*, \forall i \in F; \qquad \mu_i < \mu^*, \forall i \notin F; \tag{21}$$

$$\rho_i = \rho^*, \forall i \in D; \qquad \rho_i > \rho^*, \forall i \notin D. \tag{22}$$

Table 2: Necessary Conditions for NEs

$i \in$	D	$F \backslash D$	$\overline{F}$
m_i	$[0, \frac{r_i}{w_i r_i + C_i^A}]$	$[0, \frac{r_i}{w_i r_i + C_i^A}]$	0
p_i	$[\frac{C_i^D}{r_i w_i}, 1]$	1	1
μ_i	μ^*	μ^*	$< \mu^*$
ρ_i	ρ^*	$> \rho^*$	$+\infty$

The following theorem provides a full characterization of the set of NEs of the game.

Theorem 3. *Any pair of strategies (m, p) with $F(p) = F$ and $D(m, p) = D$ is an NE iff it is a solution to one of the following sets of constraints in addition to* (17) *to* (22)*.*

1. $\sum_{i \in F} m_i = B$; $\rho^* = 0$;
2. $\sum_{i \in F} m_i = B$; $\rho^* > 0$; $\sum_{i \in F} m_i w_i p_i = M$;
3. $\sum_{i \in F} m_i = B$; $\rho^* > 0$; $p_i = 1, \forall i \in F$;
4. $\sum_{i \in F} m_i < B$; $\mu^* = 0$; $F = F_N$; $\rho^* = 0$;
5. $\sum_{i \in F} m_i < B$; $\mu^* = 0$; $F = F_N$; $\rho^* > 0$; $\sum_{i \in F} m_i w_i p_i = M$;
6. $\sum_{i \in F} m_i < B$; $\mu^* = 0$; $F = F_N$; $\rho^* > 0$; $p_i = 1, \forall i \in F$.

Proof. We first consider the cases when the budget constraint of the defender is tight, i.e., $\sum_{i \in F} m_i = B$ (cases 1-3). Since $m_i \leq \frac{r_i}{w_i r_i + C_i^A}$ in any NE by Lemma 4 and $m_i = 0$ for i not in F by Lemma 5, we must have $B \leq \sum_{i \in F} \frac{r_i}{w_i r_i + C_i^A}$ in any NE. If $B = \sum_{i \in F} \frac{r_i}{w_i r_i + C_i^A}$, we have $\rho^* = 0$ (**case 1**). Assume $B < \sum_{i \in F} \frac{r_i}{w_i r_i + C_i^A}$. First consider the case $D = F$. We then have $m_i \leq \frac{r_i}{w_i r_i + C_i^A}, i \in F$. Hence, $\rho^* > 0$ since $B < \sum_{i \in F} \frac{r_i}{w_i r_i + C_i^A}$. It follows that $\sum_{i \in F} m_i w_i p_i = M$ (**case 2**) unless $p_i = 1, \forall i \in F$ (**case 3**); otherwise, some $p_i, i \in F$ can be increased to get more benefit. Note that case 3 can happen only if $r_i w_i - C_i^D$ is the same for all $i \in F$. Next consider the case $D \subsetneq F$. If $B \in [\sum_{i \in E} \frac{r_i}{w_i r_i + C_i^A},$

$\sum_{i\in F}\frac{r_i}{w_i r_i + C_i^A}$), we again have $\rho^* = 0$ and get case 1, but with extra constraints regarding $i \in F\backslash D$ as required by (18) and (**??**). Otherwise, if $B < \sum_{i\in D}\frac{r_i}{w_i r_i + C_i^A}$, by applying a similar argument as above, we again have $\rho^* > 0$ and get case 2 or case 3 depending on whether the attacker's budget constraint is tight or not.

We next consider the cases when $\sum_{i\in F} m_i < B$ (cases 4-6). We first observe that $p_i = \frac{C_i^D}{r_i w_i}, \forall i \in F$, or equivalently, $\mu^* = 0$. Otherwise, if $\mu_i > 0$, m_i can be further increased to reduce the cost due to the fact that $m_i \leq \frac{r_i}{r_i w_i + C_i^A} < \frac{1}{w_i}$ in any NE (by Lemma 4 and the assumption that $C_i^A > 0$), a contradiction. We then have $F = F_N$ by its definition. Cases 4-6 then follow from a similar argument for cases 1-3 by distinguishing different values of ρ^*. □

In the following, NEs that fall into each of the six cases considered above are named as Type 1 - Type 6 NEs, respectively. The next theorem shows that our game has at least one equilibrium and may have more than one NE.

Theorem 4. *The attacker-defender game always has a pure strategy Nash Equilibrium, and may have more than one NE of different payoffs to the defender.*

Proof. To show the first part, for any given index $h \leq N$, we define a pair of strategies (m^h, p^h) as follows. Let $m_i^h = 0, \forall i > h$ and let $\{m_i^h, i \leq h\}$ be the solution to the constraints (1) $\sum_{i\leq h} m_i^h = B$ and (2) ρ_i is a constant for all $i \leq h$; $p_i^h = 1, \forall i > h$ (hence $\mu_{h+1} = r_{h+1}w_{h+1} - C_h^D$), and $\forall i \leq h, p_i^h = \frac{\mu_{h+1} + C_i^D}{r_i w_i}$ if $h < N$, $p_i^h = 0$ otherwise.

We first prove the following claim. For a given h, let $h' \leq h$ denote the smallest index such that $r_{h'}w_{h'} - C_{h'}^D = r_h w_h - C_h^D$. Consider two pairs of strategies (m^h, p^h) and $(m^{h'}, p^{h'})$. We claim that if $\sum_{i\leq h} m_i^h w_i p_i^h < M$ and $\sum_{i\leq h} m_i^{h'} w_i p_i^{h'} \geq M$, then there is a Type 2 NE respecting F_h. Note that by definition, $\sum_{i\leq h} m_i^h w_i p_i^h < M$ is always true when $h = N$.

To prove the claim, we consider another pair of strategies $(m^h, p^{h'})$. If we have $\sum_{i\leq h} m_i^h w_i p_i^{h'} \geq M$, then since $\sum_{i\leq h} m_i^h w_i p_i^h < M$, there must exist p with $p_i = 1, \forall i > h$, $p_h \in [\frac{\mu_{h+1} + C_h^D}{r_h w_h}, 1]$, and $p_i = \frac{\mu_h + C_i^D}{r_i w_i}, \forall i \leq h$ such that $\sum_{i\leq h} m_i^h w_i p_i = M$. Hence, (m^h, p) is a Type 2 NE. On the other hand, if $\sum_{i\leq h} m_i^h w_i p_i^{h'} < M$, then since $\sum_{i\leq h} m_i^{h'} w_i p_i^{h'} \geq M$, there must exist m with $m_i = 0, \forall i > h$, $m_i \in [0, m_i^h], \forall h' \leq i \leq h$, and $\{m_i^h, i \leq h\}$ be the solution to the constraints (1) $\sum_{i\leq h} m_i^h = B$ and (2) ρ_i is a constant for all $i < h'$, such that $\sum_{i\leq h} m_i w_i p_i^{h'} = M$. We again get a Type 2 NE.

We then prove the theorem. First note that if $B \geq \sum_{i\leq N}\frac{r_i}{w_i r_i + C_i^A}$, then there is a Type 1 or Type 4 NE in F_N. Assume $B < \sum_{i\leq N}\frac{r_i}{w_i r_i + C_i^A}$. There is $h < N$ such that $B < \sum_{i\leq h}\frac{r_i}{w_i r_i + C_i^A}$ and $B \geq \sum_{i<h'}\frac{r_i}{w_i r_i + C_i^A}$, where h' is defined as above. If there is an NE with respect to some $F(h''), h'' > h$, we are done. Otherwise, we have $\sum_{i\leq h} m_i^h w_i p_i^h < M$ by the claim. If $\sum_{i\leq h} m_i^h w_i p_i^{h'} \geq M$, there is a Type 2 NE as proved above. Otherwise, consider the pair of strategies $(m', p^{h'})$ where $m'_i = 0, \forall i > h$, $m_i = \frac{r_i}{w_i r_i + C_i^A}, \forall i < h'$, and $\{m_i^h, i \leq h\}$ is the solution to the constraints (1) $\sum_{i \leq h} m_i^h = B$ and (2) ρ_i is a constant for all $i < h'$. If $\sum_{i \leq h} m'_i w_i p_i^{h'} \geq M$, there is Type 2 NE. Otherwise, there must be a Type 1 NE.

To show the second part, consider the following example with two nodes where $r_1 = r_2 = 1, w_1 = 2, w_2 = 1, C_1^D = 1/5, C_2^D = 4/5, C_1^A = 1, C_2^A = 7/2, B = 1/3$, and $M = 1/5$. It is easy to check that $m = (1/6, 1/6)$ and $p = (3/20, 9/10)$ is a Type 2 NE, and $m = (1/3, 0)$ and $p = (p_1, 1)$ with $p_1 \in [1/5, 3/10]$ are all Type 1 NEs, and all these NEs have different payoffs to the defender. □

5 Sequential Game

In this section, we study a sequential version of the simplified game considered in the last section. In the simultaneous game we considered in the previous section, neither the defender nor the attacker can learn the opponent's strategy in advance. While this is a reasonable assumption for the defender, an advanced attacker can often observe and learn defender's strategy before launching attacks. It therefore makes sense to consider the setting where the defender first commits to a strategy and makes it public, the attacker then responds accordingly. Such a sequential game can actually provide defender higher payoff comparing to a Nash Equilibrium since it gives the defender the opportunity of deterring the attacker from moving. We again focus on non-adaptive strategies, and further assume that at $t = 0$, the leader (defender) has determined its strategy, and the follower (attacker) has learned the defender's strategy and determined its own strategy in response. In addition, the players do not change their strategies thereafter. Our objective is to identify the best sequential strategy for the defender to commit to, in the sense of subgame perfect equilibrium [19] defined as follows. We again focus on the case where w_i is deterministic for all i.

Definition 3. *A pair of strategies $(m^\star, p^\star)$ is a subgame perfect equilibrium of the simplified game (15) and (16) if $m^\star$ is the optimal solution of*

$$\begin{aligned} \max_{m_i} & \sum_{i=1}^{N} [m_i (r_i w_i p_i^\star - C_i^D) - p_i^\star r_i] \\ s.t. & \sum_{i=1}^{N} m_i \leq B \\ & 0 \leq m_i \leq \frac{1}{w_i}, \forall i \end{aligned} \tag{23}$$

where $p_i^\star$ is the optimal solution of

$$\begin{aligned} &\max_{p_i} \sum_{i=1}^{N} p_i[r_i - m_i(r_i w_i + C_i^A)] \\ &s.t. \quad \sum_{i=1}^{N} m_i w_i p_i \leq M \\ &\qquad\quad 0 \leq p_i \leq 1, \forall i \end{aligned} \tag{24}$$

Note that in a subgame perfect equilibrium, $p_i^\star$ is still the optimal solution of (16) as in a Nash Equilibrium. However, defender's best strategy $m_i^\star$ is not necessarily optimal with respect to (15). Due to the multi-node setting and the resource constraints, it is very challenging to identify an exact subgame perfect equilibrium strategy for the defender. To this end, we propose a dynamic programming based algorithm that finds a nearly optimal defense strategy.

Remark 1. Since for any given defense strategy $\{m_i\}$, the attacker's problem (24) is a fractional knapsack problem, the optimal $p_i, \forall i$ has the following form: Sort the set of nodes by $\rho_i(m_i) = \frac{r_i - m_i(r_i w_i + C_i^A)}{m_i w_i}$ non-increasingly, then there is an index k such that $p_i = 1$ for the first k nodes, and $p_i \leq 1$ for the $k+1$-th node, and $p_i = 0$ for the rest nodes. However, if $\rho_i = \rho_j$ for some $i \neq j$, the optimal attack strategy is not unique. When this happens, we assume that the attacker always breaks ties in favor of the defender, a common practice in Stackelberg security games [13].

Before we present our algorithm to the problem, we first establish the following structural properties on the subgame perfect equilibria of the game.

Lemma 7. *In any subgame perfect equilibrium (m, p), the set of nodes can be partitioned into the following four disjoint sets according to the attack and defense strategies applied:*

1. $F = \{i | m_i > 0,\ p_i = 1\}$
2. $D = \{i | m_i > 0,\ 0 < p_i < 1\}$;
3. $E = \{i | m_i > 0,\ p_i = 0\}$;
4. $G = \{i | m_i = 0,\ p_i = 1\}$.

Moreover, they satisfy the following properties:

1. $F \cup D \cup E \cup G = \{i | i = 1, ..., n\}$ *and* $|D| \leq 1$
2. $\rho_i \geq \rho_k \geq \rho_j$ *for* $\forall i \in F,\ k \in D,\ j \in E$

Proof. It is obvious that F, D, E and G are disjoint. The three properties follow directly from the structure of the optimal solution to the attacker's problem and the remark made above. □

Since the set D has at most one element, we use m_d to represent $m_i, i \in D$ for simplicity, and let $\rho_d = \rho(m_d)$. If D is empty, we pick any node i in F with minimum ρ_i and treat it as a node in D.

Lemma 8. *For any given nonnegative ρ_d, the optimal solution for (23)-(24) satisfy the following properties:*

1. $r_i w_i - C_i^D > 0 \ \forall i \in F \cup E \cup D$
2. $m_i \le \overline{m}_i \ \forall i \in F$
3. $m_j = \overline{m}_j \ \forall j \in E$
4. $\overline{m}_i \le \frac{1}{w_i} \ \forall i$
5. $B - \sum_{i \in E} \overline{m}_i - m_d > 0.$

where $\overline{m}_i = m_i(\rho_d)$ and $m_i(\cdot)$ is the reverse function of $\rho_i(\cdot)$

Proof. If $r_i w_i - C_i^D \le 0 \ \forall i \in F \cup E \cup D$. there is no point for the defender to defend such node which will only make the payoff even worse due to high defending cost. Thus, all the nodes whose $r_i w_i - C_i^D \le 0$ are only in set G. Then, for $\forall i \in F$, $\rho_i(\overline{m}_i) = \rho_d$ and $\rho_i(m_i) \ge \rho_d$. According to the reverse relationship between ρ and m_i, we have $m_i \le \overline{m}_i$. For $\forall j \in E$, since $\rho_j(\overline{m}_j) = \rho_d$ and $\rho_j(m_j) \le \rho_d$, $\overline{m}_j$ is actually a lower bound for m_j. Setting $m_j = \overline{m}_j$ makes the cost from node i, which is $m_i C_i^D$ gets its minimum and so does the whole problem since it also uses the minimum budget from B. Therefore, more budget can be allocated for $m_i \ i \in F$ to minimize the cost from the nodes in set F. Further, it's easy to check $\overline{m}_i$ is always less than $\frac{1}{w_i}$ for any given nonnegative ρ_d. As to the 5th property, if $B - \sum_{i \in E} \overline{m}_i - m_d \le 0$, there is no budget for nodes in set F and D, which means F and D are both empty. According to the greedy method, it only happens when $M = 0$ which violates our assumption. Therefore, $B - \sum_{i \in E} \overline{m}_i - m_d > 0$. □

Remark 2. If $\rho_d < 0$, the defender can give less budget to the corresponding node to bring ρ_d down to 0. In any case, the payoffs from nodes in set D and E are 0 since the attacker will give up attacking the nodes in set D and E. Thus, the defender has more budget to defend the nodes in set F and G which brings him more payoffs. Therefore we only need to consider nonnegative ρ_d.

Lemma 9. *There exists an optimal solution vector with at most* $\min\{2, n\}$ *fractional values in 2-D fractional knapsack problem, where n is the number of variables in the knapsack problem.*

A proof of this result can be found in Chapter 9 of [12].

Lemma 10. *For any nonnegative ρ_d, there exists an optimal solution for (23)-(24) such that $\forall i \in F$, there are at most two $m_i < \overline{m}_i$ and all the other $m_i = \overline{m}_i$*

Proof. Suppose the set allocation and ρ_d are fixed, which means m_d and $\overline{m}_i \ \forall i$ are also fixed. According to Lemma 7 and Lemma 8, we can now convert (23)-

(24) to the following problem:

$$
\begin{aligned}
\min_{m_i, i\in F} & \sum_{i\in F}[r_i(1-m_iw_i)+m_iC_i^D]+\sum_{i\in G}r_i+\sum_{i\in E}\overline{m}_iC_i^D \\
& +pr_d(1-w_dm_d)+m_dC_d^D \\
s.t. & \sum_{i\in F}m_i \le B-\sum_{i\in E}\overline{m}_i-m_d \\
& \sum_{i\in F}w_im_i+pw_dm_d \le M \\
& 0\le m_i\le \overline{m}_i \ \forall i\in F
\end{aligned}
\tag{25}
$$

where $p=\min\{1,\frac{M-\sum_{i\in F}w_im_i}{w_dm_d}\}$.
It is important to note that, if $p=1$, it means all the nodes are in set F. Otherwise, such (m,p) will violates the structure of the greedy method's solution of (24). Then, (25) becomes a 2-D fractional knapsack problem with variables $\{m_i\}_{i\neq D}$. According to Lemma 9, there exists an optimal solution with at most two fractional variables which means at most two $m_i<\overline{m}_i$.

If $p=\frac{M-\sum_{i\in F}w_im_i}{w_dm_d}$, we can put p back into the target function of (25) and convert it to

$$
\begin{aligned}
\min_{m_i, i\in F} & \sum_{i\in F}[r_i(1-m_iw_i)+m_iC_i^D]+\sum_{i\in G}r_i+\sum_{i\in E}\overline{m}_iC_i^D \\
& +\frac{M-\sum_{i\in F}w_im_i}{w_dm_d}r_d(1-w_dm_d)+m_dC_d^D \\
s.t. & \sum_{i\in F}m_i \le B-\sum_{i\in E}\overline{m}_i-m_d \\
& 0\le m_i\le \overline{m}_i \ \forall i\in F
\end{aligned}
\tag{26}
$$

It is easy to see that (26) is a fractional knapsack problem. Thus, there is at most one fractional variable which means at most one $m_i<\overline{m}_i$. □

From the above lemmas, we can establish the following results about the structure of the optimal solution for (23)-(24).

Proposition 1. *For any nonnegative ρ_d, there exists an optimal solution $\{m_i\}_{i=1}^n$ such that*

1. *$\forall i\in F$, there are at most two $m_i<\overline{m}_i$ and all the other $m_i=\overline{m}_i$;*
2. *$m_d=\overline{m}_d$*
3. *$\forall i\in E$, $m_i=\overline{m}_i$;*
4. *$\forall i\in G$, $m_i=0$.*

According to Proposition 1, for any nonnegative ρ_d, once the set allocation is determined, the value of m_i can be immediately determined for all the nodes except the two fractional nodes in set F. Further, for the two fractional nodes, their m_i can be found using linear programming as discussed below. From these observations, we can convert (23)-(24) to (27) for any given nonnegative ρ_d, d, f_1 and f_2.

$$\begin{aligned} \max_{p,m_{f_1},m_{f_2},E,F,G} \quad & \sum_{i\in F\setminus\{f_1,f_2\}} [\overline{m}_i(r_iw_i - C_i^D) - r_i] + \sum_{j=1}^{2}[m_{f_j}(r_{f_j}w_{f_j} - C_{f_j}^D) - r_{f_j}] \\ & - \sum_{i\in G} r_i - \sum_{i\in E} \overline{m}_i C_i^D + m_d(pr_dw_d - C_d^D) - pr_d \\ s.t. \quad & \sum_{i\in F\setminus\{f_1,f_2\}} \overline{m}_i + m_{f_1} + m_{f_2} + \sum_{i\in E}\overline{m}_i + m_d \le B \\ & \sum_{i\in F\setminus\{f_1,f_2\}} w_i\overline{m}_i + w_{f_1}m_{f_1} + w_{f_2}m_{f_2} + pw_dm_d \le M \\ & 0 \le m_{f_1} \le \overline{m}_1,\ 0 \le m_{f_2} \le \overline{m}_2,\ 0 \le p \le 1 \end{aligned} \tag{27}$$

Note that, the set allocation is part of the decision variables in (27).

We then propose the following algorithm to the defender's problem (see Algorithm 1). The algorithm iterates over nonnegative ρ_d (with a step size ρ_{step}) (lines 3-10). For each ρ_d, it iterates over all possible node d in set D, and all possible nodes f_1, f_2 with fractional assignment in set F (lines 5-8). Given ρ_d, d, f_1, f_2, the best set allocation (together with m_i for all i and p) are determined using dynamic programming as explained below (lines 6-7), where we first assume that B, M, $\overline{m}_i$ and w_i have been rounded to integers for all i . The loss of performance due to rounding will be discussed later.

Consider any ρ_d, node d is in set D, and nodes f_1, f_2 with frictional assignment in set F. Let $SEQ(i, b, m, d, f_1, f_2, ind)$ denote the maximum payoff of the defender considering only node 1 to node i (excluding nodes d, f_1 and f_2), for given budgets b and m for the two constraints in (27), respectively. The ind is a boolean variable that indicates whether the second constraint of (27) is tight for node 1 to i. If ind is $True$, it means all the budget m is used up for node 1 to i. ind is $False$ meaning that there is still budget m available for the attacker. Here, $0 \le b \le B$ and $0 \le m \le M$. The value of $SEQ(i, b, m, d, f_1, f_2, ind)$ is determined recursively as follows. If $b < 0$ or $m < 0$, the value is set to $-\infty$. If node i is one of d, f_1 and f_2, we simply set $SEQ(i, b, m, d, f_1, f_2, ind) = SEQ(i-1, b, m, d, f_1, f_2, ind)$. Otherwise, we have the following recurrence equation, where the three cases refer to the maximum payoff when putting nodes i in set F, E, and G, respectively.

$$\begin{aligned} & SEQ(i, b, m, d, f_1, f_2, ind) \\ & = \max\Big\{SEQ(i-1, b-\overline{m}_i, m - w_i\overline{m}_i, d, f_1, f_2, ind) + \overline{m}_i(r_iw_i - C_i^D) - r_i, \\ & SEQ(i-1, b-\overline{m}_i, m, d, f_1, f_2, ind) - \overline{m}_iC_i^D, SEQ(i-1, b, m, d, f_1, f_2, ind) - r_i\Big\} \end{aligned} \tag{28}$$

Meanwhile, if ind is $False$, node i can be allocated to set E only if $r_i - \overline{m}_i(r_iw_i + C_i^A) \le 0$. Otherwise, there is still available budget for the attacker to attack other nodes with reward greater than 0 which violates the structure of the greedy solution for (24). Also, if ind is $False$, it means m is not used up. Thus we should return $-\infty$ if ind is $False$, $i > 0$ and $m = 0$.

Moreover, we let $SEQ(0, b, m, d, f_1, f_2, ind)$ denote the maximum defense payoff when only nodes in d, f_1, and f_2 are considered. If ind is $True$, the following linear program in (29) determines the optimal values of p, m_{f_1} and m_{f_2} for given budgets b and m:

$$\begin{aligned} \max_{m_{f_i}, m_{f_2}} \ & \sum_{j=1}^{2} [m_{f_j}(r_{f_j} w_{f_j} - C_{f_j}^D) - r_{f_j}] + m_d(p r_d w_d - C_d^D) - p r_d \\ s.t. \ & m_{f_1} + m_{f_2} + m_d \leq b \\ & m_{f_1} w_{f_1} + m_{f_2} w_{f_2} \leq m \\ & m_{f_1} \leq \overline{m}_{f_1}, \quad m_{f_2} \leq \overline{m}_{f_2} \\ & p = \frac{m - m_{f_1} w_{f_1} - m_{f_2} w_{f_2}}{w_d m_d} \leq 1 \end{aligned} \tag{29}$$

If ind is $False$, we must have $p = 1$. The optimal values of m_{f_1} and m_{f_2} are determined by (30):

$$\begin{aligned} \max_{m_{f_i}, m_{f_2}} \ & \sum_{j=1}^{2} [m_{f_j}(r_{f_j} w_{f_j} - C_{f_j}^D) - r_{f_j}] + m_d(r_d w_d - C_d^D) - r_d \\ s.t. \ & m_{f_1} + m_{f_2} + m_d \leq b \\ & m_{f_1} w_{f_1} + m_{f_2} w_{f_2} \leq m - w_d m_d \\ & m_{f_1} \leq \overline{m}_{f_1}, \quad m_{f_2} \leq \overline{m}_{f_2} \end{aligned} \tag{30}$$

Algorithm 1 Sequential Strategy for Defender

```
Initialize $\rho_{step}$
$\rho_{max} \leftarrow \min\{\rho : \sum_{i=1}^{n} w_i m_i(\rho) \leq M\}$
for $\rho_d \leftarrow 0$ to $\rho_{max}$ with step size $\rho_{step}$ do
    $\overline{m}_i \leftarrow m_i(\rho_d)$ for all $i$
    for $d, f_1, f_2 \leftarrow 1$ to $n$ do
        $val_{d,f_1,f_2} \leftarrow SEQ(n, B, M, d, f_1, f_2, True)$
        $val'_{d,f_1,f_2} \leftarrow SEQ(n, B, M, d, f_1, f_2, False)$
    end for
    $C_{dp}(\rho_d) \leftarrow \max_{d,f_1,f_2}\{val_{d,f_1,f_2}, val'_{d,f_1,f_2}\}$
end for
$C^{\star}_{alg} \leftarrow \max_{\rho_d}\{C_{dp}(\rho_d)\}$
```

Since the dynamic program searches for all the possible solutions that satisfy Proposition 1, $C_{dp}(\rho_d)$ gives us the optimal solution of (23)-(24) for any given nonnegative ρ_d. Algorithm 1 then computes the optimal solution by searching all the nonnegative ρ_d. Note that d, f_1 and f_2 can be equal to include the case that there is only one or zero node in set F. The minimum possible value of

ρ is 0 (explained in Remark 2). The maximum possible value of ρ is $\min\{\rho : \sum_{i=1}^{n} w_i m_i(\rho) \leq M\}$. For larger ρ, the sum of all $w_i \overline{m}_i$ will be less than M. In this case, all the nodes will be in set F and $p_i = 1\ \forall i$, which makes (23)-(24) a simple knapsack problem that can be easily solved.

Additionally, since the dynamic program searches over all feasible integer values, we use a simple rounding technique to guarantee it is implementable. Before the execution of $SEQ(n, B, M, d, f_1, f_2, ind)$, we set $\overline{m}_i \leftarrow \lfloor \frac{\overline{m}_i}{\delta} \rfloor$, $w_i \leftarrow \lfloor \frac{w_i}{\delta} \rfloor$ for all i and $B \leftarrow \lfloor \frac{B}{\delta} \rfloor$, $M \leftarrow \lfloor \frac{M}{\delta} \rfloor$ where δ is an adjustable parameter. Intuitively, by making δ and ρ_{step} small enough, Algorithm 1 can find a strategy that is arbitrarily close to the subgame perfect equilibrium strategy of the defender. Formally, we can establish the following result.

Lemma 11. *For any ϵ, if $\rho_{step} \leq \frac{\epsilon}{\Lambda}$, we have $\frac{|C_{alg}|}{|C^\star|} \leq 1 + \epsilon$ where C_{alg} is the payoffs of the strategy found by Algorithm 1, $C^\star$ is the optimal payoff and $\Lambda = \max_i\{\frac{w_i}{C_i^D}\} + (\frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}} + \max_i\{r_i + \frac{C_i^A}{w_i}\}) \cdot \max_i\{\frac{1}{r_i^2} \cdot \max\{1, (\frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}} + r_i)\frac{w_i}{C_i^D} + \frac{C_i^A}{C_i^D}\}\}$*

Proof. Denote $\rho^\star$ as the optimal ρ_d for computing $C^\star$ and ρ' is the first ρ_d which is greater than $\rho^\star$ in Algorithm 1. Then we have

$$\begin{aligned} \triangle m_i &= \frac{r_i}{(\rho^\star + r_i)w_i + C_i^A} - \frac{r_i}{(\rho' + r_i)w_i + C_i^A} \\ &\leq \frac{(\rho' - \rho^\star) r_i w_i}{[(\rho^\star + r_i)w_i + C_i^A]^2} \leq \frac{\rho_{step} r_i w_i}{[(\rho^\star + r_i)w_i + C_i^A]^2} \end{aligned} \tag{31}$$

In addition, we have $\frac{r_i}{(\rho_{max} + r_i)w_i + C_i^A} \leq \overline{m}_i \leq \frac{r_i}{r_i w_i + C_i^A}$ for any ρ_d and i. Now, we consider one particular solution for ρ' in which the set allocation is the same as the optimal solution of (23) but each m_i decrease $\triangle m_i$. Thus, the cost increases in two parts due to the decrease of m_i. The first part is from those nodes in F and the seconde part comes from the extra budget for the attacker to attack those nodes in set D and E. Let $\overline{m}_i = m_i(\rho^\star)$ and $\overline{m}_i' = m_i(\rho')$. It follows that

$$\begin{aligned} \frac{|C_{alg}| - |C^\star|}{|C^\star|} &\leq \frac{\sum_{i \in F \cup D} \triangle m_i (r_i w_i - C_i^D) + (\sum_{i=1}^{n} \triangle m_i w_i) \cdot \max_i\{\frac{r_i(1 - w_i \overline{m}_i')}{w_i \overline{m}_i'}\}}{C^\star} \\ &\leq \frac{\sum_{i \in F \cup D} \rho_{step} \frac{r_i w_i (r_i w_i - C_i^D)}{[(\rho^\star + r_i)w_i + C_i^A]^2} + (\sum_{i=1}^{n} \rho_{step} \frac{r_i w_i^2}{[(\rho^\star + r_i)w_i + C_i^A]^2}) \cdot \max_i\{\frac{r_i(1 - w_i \overline{m}_i')}{w_i \overline{m}_i'}\}}{C^\star} \\ &\leq \rho_{step} \cdot \left(\frac{\sum_{i \in F \cup D} \overline{m}_i^2 (r_i w_i - C_i^D) w_i / r_i}{\sum_{i \in F \cup D} [r_i(1 - \overline{m}_i w_i) + \overline{m}_i C_i^D]} + \frac{\sum_{i=1}^{n} (\overline{m}_i w_i)^2 / r_i \cdot \max_i\{\frac{r_i}{w_i \overline{m}_i'}\}}{\sum_{i \in F \cup D \cup E} \overline{m} C_i^D + \sum_{i \in G} r_i} \right) \\ &\leq \rho_{step} \left(\max_i\{\frac{\overline{m}_i w_i (r_i w_i - C_i^D)}{r_i C_i^D}\} + \frac{\sum_{i=1}^{n} (1/r_i)^2 \cdot \max_i\{\rho_{max} + r_i + \frac{C_i^A}{w_i}\}}{\sum_{i \in F \cup D \cup E} \frac{r_i C_i^D}{(\rho_{max} + r_i)w_i + C_i^A} + \sum_{i \in G} r_i} \right) \\ &\leq \rho_{step} \left(\max_i\{\frac{w_i}{C_i^D}\} + \max_i\{\frac{1}{r_i^2}, \frac{(\rho_{max} + r_i)w_i + C_i^A}{r_i^2 C_i^D}\} \cdot \max_i\{\rho_{max} + r_i + \frac{C_i^A}{w_i}\} \right) \end{aligned} \tag{32}$$

Further, according to the definition of ρ_{max} in Algorithm 1, we have $\rho_{max} \leq \frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}}$. Put it in (33) and we get

$$\frac{|C_{alg}|}{|C^\star|} = 1 + \frac{|C_{alg}| - |C^\star|}{|C^\star|} \leq 1 + \rho_{step} \cdot \varLambda \leq 1 + \epsilon \tag{33}$$

□

Based on Lemma 11, we have the following theorem

Theorem 5. *For any ϵ, if $\rho_{step} \leq \frac{\epsilon}{2\varLambda}$ and $\delta \leq \frac{\epsilon}{2\varPsi}$ we have $\frac{|C_{alg}|}{|C^\star|} \leq 1 + \epsilon$ where $\varPsi = \max_i\{\frac{w_i^2}{C_i^D} \cdot (\frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}} + r_i + \frac{C_i^A}{w_i})\} + (\frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}} + \max_i\{r_i + \frac{C_i^A}{w_i}\}) \cdot \max_i\{\frac{w_i}{r_i} \cdot \max\{1, (\frac{n \min_i\{r_i w_i\}}{M \max_i\{w_i\}} + r_i)\frac{w_i}{C_i^D} + \frac{C_i^A}{C_i^D}\}\}$*

The proof is similar to that in Lemma 11. The only difference is the decrease of m_i due to rounding. Adding the loss of rounding, we have $\triangle m_i \leq \frac{\rho_{step} r_i w_i}{[(\rho^\star + r_i)w_i + C_i^A]^2} + \delta$. Put it into (33) and we get $\frac{|C_{alg}|}{|C^\star|} \leq 1 + \rho_{step} \cdot \varLambda + \delta \cdot \varPsi \leq 1 + \epsilon$

To find $SEQ(n, B, M, d, f_1, f_2, ind)$, the dynamic program searches over all possible values of $i \in \{0, ..., n\}$, $b \leq B$ and $m \leq M$. Thus, the total time complexity for the dynamic programming is $O(\frac{n^3 BM}{\epsilon^2})$, and the time complexity for Algorithm 1 is $O(\frac{n^8 BM}{\epsilon^3})$

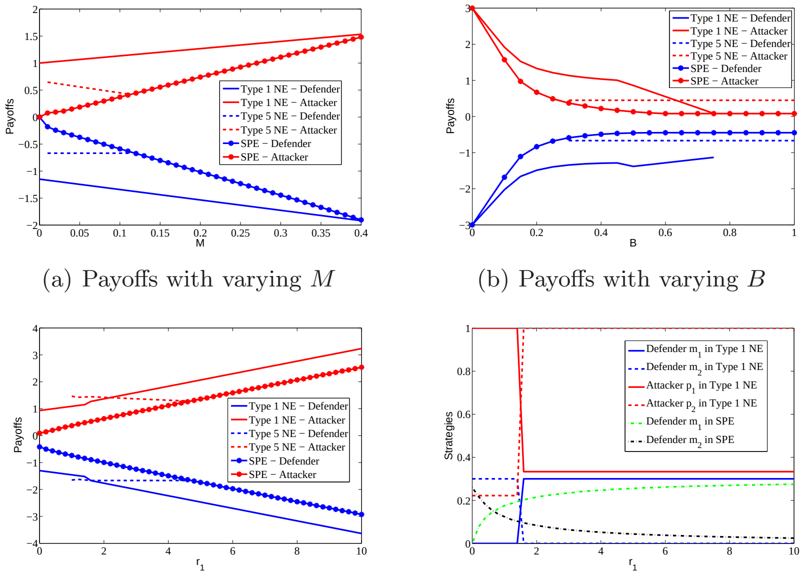
6 Numerical Result

In this section, we present numerical results for our game models. For the illustrations, we assume that all the attack times w_i are deterministic as in Sections 4 and 5. We study the payoffs of both attacker and defender and their strategies in both Nash Equilibrium and subgame perfect equilibrium in a two-node setting, and study the impact of various parameters including resource constraints B, M, and the unit value r_i. We further study the payoffs and strategies for both players in subgame perfect equilibrium in a five-node setting, and study the impact of various parameters.

We first study the impact of the resource constraints M, B, and the unit value r_1 on the payoffs for the two node setting in Figure 2. In the figure, we have plotted both Type 1 and Type 5 NE [4] and subgame perfect equilibrium. Type 5 NE only occurs when M is small as shown in Figure 2(a), while Type 1 NE appears when B is small as shown in Figure 2(b), which is expected since B is fully utilized in a Type 1 NE while M is fully utilized in a Type 5 NE. When the defense budget B becomes large, the summation of m_i does not necessarily equal to B and thus Type 1 NE disappears. Similarly, the Type 5 NE disappears for large attack budget M. In Figures 2(c) and 2(d), we vary the unit value of node 1, r_1. At the beginning, the defender protects node 2 only since $w_2 > w_1$. As r_1 becomes larger and larger, the defender starts to change

[4] There are also Type 2 NE, which are omitted for the sake of clarify.

its strategy by protecting node 1 instead of node 2 in NE Type 1. On the other hand, since node 1 is fully protected by the defender and the defender gives up defending node 2, the attacker begins to attack node 2 with probability 1, and uses the rest budget to attack node 1 with probability less than 1, due to the high defending frequency and limited resources M. We further observe that in both the simultaneous game and the sequential game, the value of m_1 increases along with the increase of r_1, while the value of m_2 decreases at the same time. This implies that that the defender tends to protect the nodes with higher values more frequently. In addition, the subgame perfect equilibrium always bring the defender higher payoffs compared with Nash Equilibrium, which is expected.



(a) Payoffs with varying M

(b) Payoffs with varying B

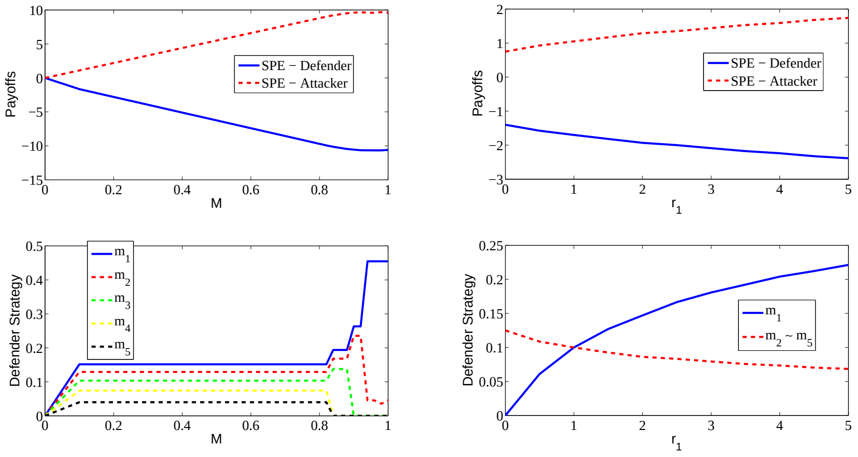
(c) Payoffs with varying r_1

(d) Strategies with varying r_1

Fig. 2: The effects of varying resource constraints, where in all the figures, $r_2 = 1, w_1 = 1.7, w_2 = 1.6, C_1^D = 0.5, C_2^D = 0.6, C_1^A = 1, C_2^A = 1.5$, and $r_1 = 2$ in (a) and (b), $B = 0.3$ in (a), (c), and (d), and $M = 0.1$ in (b), (c), and (d).

Moreover, it it interesting to observe that under the Type 5 NE, the attacker's payoff decreases for a larger M as shown in Fig 2(a). This is because the defender's budget B is not fully utilized in Type 5 NE, and the defender can use more budget to protect both nodes when M increases. The increase of the attacker's payoff by having a larger M is canceled by the increase of the defender's move frequency m_1 and m_2. We also note that the Type 5 NE is less preferable for the defender in Figure-2(c) when r_1 is small and favors defender as r_1 increases, which tells us that the defender may prefer different types of NEs under different scenarios and so does the attacker.

We then study the effects of varying M and r_1 on both players' payoffs and strategies in the sequential game for the five-node setting. In Figure 3(a), the



(a) Payoffs and strategies with varying M (b) Payoffs and strategies with varying r_1

Fig. 3: The effects of varying resource constraints and r_1, where $w = [2\ 2\ 2\ 2\ 2]$, $C^D = C^A = [1\ 1\ 1\ 1\ 1]$, $B = 0.5$, $r = [5\ 4\ 3\ 2\ 1]$ in (a), $r = [r_1\ 1\ 1\ 1\ 1]$ and $M = 0.3$ in (b).

parameters of all the nodes are the same except r_i. We vary the attacker's budget M from 0 to 1. When $M = 0$, the defender can set m_i for all i to arbitrary small (but positive) values, so that the attacker is unable to attack any node, leading to a zero payoff for both players. As M becomes larger, the attacker's payoff increases, while the defender's payoff decreases, and the defender tends to defend the nodes with higher values more frequently, as shown in Figure 3(a)(lower). After a certain point, the defender gives up some nodes and protects higher value nodes more often. This is because with a very large M, the attacker is able to attack all the nodes with high probability, so that defending all the nodes with small m_i is less effective than defending high value nodes with large m_i. This result implies that the attacker's resource constraint has a significant impact on the defender's behavior and when M is large, protecting high value nodes more frequently and giving up several low value nodes is more beneficial for the defender compared to defending all the nodes with low frequency.

In Figure 3(b), we vary r_1 while setting other parameters to be the same for all the nodes. Since all the nodes other than node 1 are identical, they have the same m_i as shown in Figure 3(b)(lower). We observe that the defender protects node 1 less frequently when r_1 is smaller than the unit value of other nodes. When r_1 becomes larger, the defender defends node 1 more frequently, which tells us the defender should protect the nodes with higher values more frequently in the subgame perfect equilibrium when all the other parameters are the same.

7 Conclusion

In this paper, we propose a two-player non-zero-sum game for protecting a system of multiple components against a stealthy attacker where the defender's behavior is fully observable, and both players have strict resource constraints. We prove that periodic defense and non-adaptive *i.i.d.* attack are a pair of best-response strategies with respect to each other. For this pair of strategies, we characterize the set of Nash Equilibria of the game, and show that there is always one (and maybe more) equilibrium, for the case when the attack times are deterministic. We further study the sequential game where the defender first publicly announces its strategy, and design an algorithm that can identify a strategy that is arbitrarily close to the subgame perfect equilibrium strategy for the defender.

References

1. Advanced persistent threat. `http://en.wikipedia.org/wiki/Advanced_persistent_threat`.
2. ESET and Sucuri Uncover Linux/Cdorked.A: The Most Sophisticated Apache Backdoor. `http://www.eset.com/int/about/press/articles/article/eset-and-sucuri-uncover-linuxcdo` `most-sophisticated-ever-affecting-thousands-of-web-sites/`, 2013.
3. A. Coviello. Open letter to RSA customers, March 17, 2011. `http://www.rsa.com/node.aspx?id=3872`.
4. T. Alpcan and T. Başar. *Network Security: A Decision and Game-Theoretic Approach*. Cambridge University Press, 2010.
5. R. Anderson. Why Information Security is Hard - An Economic Perspective. In *Proc. of ACSAC*, 2001.
6. B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi. The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 4:971–1003, 2012.
7. K. D. Bowers, M. E. V. Dijk, A. Juels, A. M. Oprea, R. L. Rivest, and N. Triandopoulos. Graph-based approach to deterring persistent security threats. US Patent 8813234, 2014.
8. K. D. Bowers, M. van Dijk, R. Grifn, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos. Defending Against the Unknown Enemy: Applying FLIPIT to System Security. In *Proc. of GameSec*, 2012.
9. L. Buttyan and J.-P. Hubaux. *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. Cambridge University Press, 2007.
10. A. Gueye, V. Marbukh, and J. C. Walrand. Towards a Metric for Communication Network Vulnerability to Attacks: A Game Theoretic Approach. In *Proc. of Gamenets*, 2012.
11. M. Kearns and L. E. Ortiz. Algorithms for Interdependent Security Games. In *Proc. of NIPS*, 2003.
12. H. Kellerer, U. Pfeschy, and D. Pisinger. *Knapsack Problems*. Springer, 2004.
13. D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe. Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness. *Journal of Artificial Intelligence Research*, 41:297–327, 2011.

14. H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3), 2003.
15. A. Laszka, G. Horvath, M. Felegyhazi, and L. Buttyán. Flipthem: Modeling targeted attacks with flipit for multiple resources. In *Proc. of GameSec*, 2014.
16. A. Laszka, B. Johnson, and J. Grossklags. Mitigating Covert Compromises: A Game-Theoretic Model of Targeted and Non-Targeted Covert Attacks. In *Proc. of WINE*, 2013.
17. M. H. Manshaei, Q. Zhu, T. Alpcan, and T. Başar. Game Theory Meets Network Security and Privacy. *ACM Computing Surveys*, 2012.
18. T. Moore and R. Anderson. Economics and internet security: a survey of recent analytical, empirical and behavioral research. `ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf`, 2011.
19. M. J. Osborne and A. Rubinstein. *A Course in Game Theory.* The MIT Press, 1994.
20. M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, 2011.
21. M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest. FlipIt: The Game of "Stealthy Takeover". *Journal of Cryptology*, 26(4):655–713, 2013.

8 Appendix

Proof of Lemma 3: In order to get the attacker's best responses against any defender's deterministic strategies, we first divide (4) into N sub-optimization problems

$$\begin{aligned} &\min_{\alpha_{i,k}} \sum_{k=1}^{L_i} \frac{E[\min(\alpha_{i,k}+w_i, X_{i,k})]r_i + P(\alpha_{i,k} < X_{i,k})C_i^A}{T} \\ &s.t. \sum_{k=1}^{L_i} \frac{E[\min(\alpha_{i,k}+w_i, X_{i,k})] - E[\min(\alpha_{i,k}, X_{i,k})]}{T} \le M_i \end{aligned} \tag{34}$$

where $\sum_{i=1}^{N} M_i = M$. Note that here we consider the equivalent minimization problem by taking the negative of the target function of (4) and omitting the constant part. We further divide each sub-problem into L_i sub-problems as follows

$$\begin{aligned} &\min_{\alpha_{i,k}} \frac{E[\min(\alpha_{i,k}+w_i, X_{i,k})]r_i + P(\alpha_{i,k} < X_{i,k})C_i^A}{T} \\ &s.t. \frac{E[\min(\alpha_{i,k}+w_i, X_{i,k})] - E[\min(\alpha_{i,k}, X_{i,k})]}{T} \le M_{i,k} \end{aligned} \tag{35}$$

where $\sum_{k=1}^{L_i} M_{i,k} = M_i$. We claim that, the optimal solution to (35) is to allocate as much budget as possible to $P(\alpha_{i,k} = 0)$, that is

$$\alpha_{i,k}^* = \begin{cases} 0 & \text{w.p. } p_{i,k}^* \\ \ge X_{i,k} & \text{w.p. } 1 - p_{i,k}^* \end{cases} \tag{36}$$

where

$$p^*_{i,k} = \begin{cases} \min(1, \quad \frac{M_{i,k}T}{E[\min(w_i, X_{i,k})]}) \\ \qquad\qquad \text{if } r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A < 0 \\ 0 \qquad\qquad \text{if } r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A \geq 0 \end{cases} \tag{37}$$

The proof of the claim is provided below. Since $M_{i,k}$ is any number such that $\sum_{k=1}^{L_i} M_{i,k} = M_i$, the optimal solution of (34) also satisfies the same structure of (36). A similar argument also applies to the optimal solution of (4), although the optimal $p_{i,k}$ are not necessarily the same as in (37). We then prove our claim. For simplicity, we assume that $\alpha_{i,k}$ is a discrete r.v., and without loss of generality, it has the following p.m.f

$$\alpha_{i,k} = \begin{cases} 0 & \text{w.p. } p_0 \\ v_1 & \text{w.p. } p_1 \\ & \vdots \\ v_n & \text{w.p. } p_n \\ \geq X_{i,k} & \text{w.p. } 1 - \sum_{j=0}^{n} p_j \end{cases} \tag{38}$$

where $n \in \mathbb{N}$ and $v_j \in \mathbb{R}$, $j = 1, ..., n$, such that $0 < v_1 < v_2 < \ldots < v_n < X_{i,k}$. We note that the following proof can be adapted to the continuous $\alpha_{i,k}$ as well by replacing sums with integrals and p.m.f with p.d.f.

From the definition of $\alpha_{i,k}$, we have

$$\begin{aligned} & E[\min(\alpha_{i,k} + w_i, X_{i,k})] \\ & = p_0 E[\min(w_i, X_{i,k})] + \sum_{j=1}^{n} p_j E[\min(v_j + w_i, X_{i,k})] + (1 - \sum_{j=0}^{n} p_j) X_{i,k} \\ & = p_0 E[\min(w_i, X_{i,k})] + \sum_{j=1}^{n} p_j E[\min(w_i, X_{i,k} - v_j)] + (1 - \sum_{j=0}^{n} p_j) X_{i,k} + \sum_{j=1}^{n} p_j v_j \end{aligned}$$

Problem (35) can then be converted to the following form

$$\begin{aligned} \min \quad & p_0(r_i[E[\min(w_i, X_{i,k})] - X_{i,k}] + C_i^A) \\ & + \sum_{j=1}^{n} p_j(r_i[E[\min(v_j + w_i, X_{i,k})] - X_{i,k}] + C_i^A) + X_{i,k} r_i \\ s.t. \quad & p_0 E[\min(w_i, X_{i,k})] + \sum_{j=1}^{n} p_j E[\min(w_i, X_{i,k} - v_i)] \leq M_{i,k} T \\ & \sum_{j=0}^{n} p_j \leq 1 \end{aligned} \tag{39}$$

where we omit the constant T in the objective function for simplicity. Let $J(\{p_0, ..., p_n\})$ denote the objective function in (39).

Since $r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A < r_i(E[\min(v_j + w_i, X_{i,k})] - X_{i,k}) + C_i^A$, if $r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A \geq 0$, $J(\{p_0, ..., p_n\})$ is minimized by setting $p_j = 0, \forall j = 0, ..., n$, which implies $\alpha_{i,k} \geq X_{i,k}$ w.p.1. Such condition describes the case that even if the attacker attacks the node immediately after it is recovered, its reward is still less than 0. Therefore, the attacker never attacks. If $r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A < 0$, we claim that the optimal solution is to allocate as much budget $M_{i,k}T$ as possible to p_0, that is, we set all $p_j = 0$, $1 \leq j \leq n$, and $p_0 = \min(1, \frac{M_{i,k}T}{E[\min(w_i, X_{i,k})]})$. This is clearly true if $r_i(E[\min(v_j + w_i, X_{i,k})] - X_{i,k}) + C_i^A \geq 0$. Therefore, it suffices to consider the case when $r_i(E[\min(w_i, X_{i,k})] - X_{i,k}) + C_i^A < r_i(E[\min(v_j + w_i, X_{i,k})] - X_{i,k}) + C_i^A < 0$.

To prove the claim, consider an optimal solution $\{p_0, p_1, ..., p_n\}$ to (39). We show that if $p_0 < \min(1, \frac{M_{i,k}T}{E[\min(w_i, X_{i,k})]})$, then we can find another optimal solution $\{p'_0, p'_1, ..., p'_n\}$ such that $p'_0 > p_0$. We distinguish the following two cases:

Case 1: $p_0 E[\min(w_i, X_{i,k})] + \sum_{j=1}^n p_j E[\min(w_i, X_{i,k} - v_i)] < M_{i,k}T$. Then by the optimality of $\{p_0, p_1, ..., p_n\}$ and the assumption that $r_i(E[\min(v_j + w_i, X_{i,k})] - X_{i,k}) + C_i^A < 0$, we must have $\sum_{j=0}^n p_j = 1$. Let $j \geq 1$ denote an index such that $p_j > 0$. Then there must exist a small amount $\triangle p > 0$ such that $p'_0 = p_0 + \triangle p, p'_j = p'_j - \triangle p, p'_k = p_k, \forall k \neq 0$ and $k \neq j$ is again a feasible solution to (39). We further have

$$\begin{aligned}
&J(\{p_0, ..., p_n\}) - J(\{p'_0, ..., p'_n\}) \\
&= \triangle p(r_i[E[\min(v_j + w_i, X_{i,k})] - X_{i,k}] + C_i^A) \\
&\quad - \triangle p(r_i[E[\min(w_i, X_{i,k})] - X_{i,k}] + C_i^A) \\
&= \triangle p r_i(E[\min(v_j + w_i, X_{i,k})] - E[\min(w_i, X_{i,k})]) \\
&\geq 0
\end{aligned}$$

Case 2: $p_0 E[\min(w_i, X_{i,k})] + \sum_{j=1}^n p_j E[\min(w_i, X_{i,k} - v_i)] = M_{i,k}T$. Again let $j \geq 1$ denote an index such that $p_j > 0$. Then there must exist a small amount $\triangle M > 0$ such that $p'_0 = p_0 + \frac{\triangle M}{E[\min(w_i, X_{i,k})]}, p'_j = p'_j - \frac{\triangle M}{E[\min(w_i, X_{i,k} - v_j)]}, p'_k = p_k, \forall k \neq 0$ and $k \neq j$ is a feasible solution to (39). We further have

$$\begin{aligned}
&J(\{p_0, ..., p_n\}) - J(\{p'_0, ..., p'_n\}) \\
&= \frac{\triangle M(r_i[E[\min(v_j + w_i, X_{i,k})] - X_{i,k}] + C_i^A)}{E[\min(w_i, X_{i,k} - v_j)]} \\
&\quad - \frac{\triangle M(r_i[E[\min(w_i, X_{i,k})] - X_{i,k}] + C_i^A)}{E[\min(w_i, X_{i,k})]} \\
&= \frac{\triangle M}{E[\min(w_i, X_{i,k} - v_j)]}(r_i v_j - r_i X_{i,k} + C_i^A) \\
&\quad - \frac{\triangle M}{E[\min(w_i, X_{i,k})]}(-r_i X_{i,k} + C_i^A) \\
&\geq 0
\end{aligned}$$

□